

TP 3 : Configuration et Administration d'un switch

Matière: RESEAUX LOCAUX

Enseignant: Ramzi BELLAZREG

Les niveaux d'accès

Par mesure de sécurité, l'IOS sépare les sessions d'exécution en trois niveaux d'accès :

- Mode exec ou utilisateur : mode avec droits restreints (>) ;
- Mode privilégié ou enable : mode de consultation de la configuration (#) ;
- Mode configuration (conf) : mode de modification de la configuration ;

- **enable** : bascule en mode privilégié avec mot de passe ;

- **configure terminal** ou **conf t** : passer à la configuration globale en indiquant que celle-ci se fera à partir du terminal ;

- **exit** : pour descendre d'un niveau de commande ;

- **CTRL-Z** ou **end** : pour sortir du mode configuration ;

Le ? permet de voir les commandes disponibles et leurs différentes options.

Manipulation des configurations

```
Switch#show running-config
```

```
Switch#show startup-config
```

```
Switch#Copy running-config startup-config //ou le contraire
```

```
Switch(config)#hostname RI-Switch //attribue un nom au switch
```

```
Switch#Show interfaces // afficher les interfaces du switch
```

```
Switch#Show interfaces identifiant_interface // affiche les informations de l'interface mentionnée
```

Configuration d'une interface

Après passage en mode configuration d'interface, vous pouvez faire plusieurs manipulations :

```
Switch(config)#interface nom_interface // passer en mode configuration de l'interface donnée
```

```
Switch(config-if)#duplex {auto|full|half} // modifie le mode duplex
```

```
Switch(config-if)#speed {auto|10|100|...} // modifie la vitesse du port
```

```
Switch(config-if)#shutdown //désactive l'interface
```

```
Switch(config-if)#no shutdown // active l'interface
```

Définition des mots de passes

Switch(config)#**enable password** *mot-passe*
Switch(config)#**enable secret** *mot-passe*

Configuration du mot de passe console	Configuration du mot de passe terminal
Switch(config)# Line console 0 Switch(config)# Password mot-passe Switch(config)# Login	Switch(config)# Line vty 0 4 Switch(config)# Password mot-passe Switch(config)# Login

Switch(config)#**Service password-encryption** // crypter les mots de passes

A partir d'une poste, vous pouvez ouvrir une session sur le switch :

- terminal console sur le port série et à l'aide du logiciel terminal. Cet outil est équivalent à l'outil HyperTerminal de Windows (Programmes > Accessoires > Communications> HyperTerminal) ;
- terminal telnet, à l'aide de la commande DOS **telnet @IP_switch** ;

Manipulation de la table MAC et ARP

Switch#**show mac-address-table** // affichage table des adresses MAC
Switch#**clear mac-address-table dynamic** //effacer la table des adresses MAC

Switch(config)#**mac-address-table static adresse-mac vlan 1 interface identifiant-interface** // ajout d'une adresse mac statique

Switch#**show arp** //afficher la table arp

Définition d'une adresse ip du switch

Switch(config)#**interface VLAN 1**
Switch(config-if)#**ip address** *adresse_IP* *masque_réseau*
Switch(config-if)# **no shutdown**
Switch(config-if)#**exit**

Les commandes de contrôle d'accès

✚ Pour éviter que n'importe qui se connecte sur les ports d'un switch, il est possible de faire un contrôle sur les adresses MAC des machines qui ont le droit de se connecter sur chaque port. Pour activer cette sécurité sur l'interface concernée :

```
Switch(config-if)# switchport mode access  
Switch(config-if)# switchport port-security
```

- ✚ La définition des adresses MAC autorisées sur un port peut se faire de deux manières différentes soit :

- ▶ **Adresse MAC fixée manuellement:**

```
Switch (config-if)# switchport port-security mac-address @MAC_autorisée
```

- ▶ **Adresse MAC (source) apprise automatiquement à partir de la première trame qui traversera le port :**

```
Switch (config-if)# switchport port-security mac-address sticky
```

- ✚ Nous pouvons Limiter le nombre d'hôtes (adresses MAC) qui peuvent accéder sur chaque port

```
RI-Switch(config-if)#switchport port-security maximum nombre_maximum
```

- ✚ Pour visualiser la politique de sécurité d'une interface, utiliser la commande suivante.

```
RI-Switch # show port-security interface nom_interface
```

- ✚ Cette commande efface la table des adresses MAC, déverrouille la sécurité des adresses MAC et permet l'enregistrement d'une nouvelle adresse.

```
RI-Switch#clear mac-address-table dynamic
```

- ✚ Pour modifier les paramètres de sécurité, vous pouvez utiliser les commandes suivantes.

- ▶ **Désactivation de la sécurité sur le port**

```
RI-Switch(config-if)#no switchport port-security
```

- ▶ **Désactivation de l'apprentissage automatique d'adresse MAC**

```
RI-Switch(config-if)#no switchport port-security mac-address sticky
```

- ▶ **Suppression d'une adresse MAC de la liste des MAC autorisées**

```
RI-Switch(config-if)#no switchport port-security mac-address 0008.744d.8ee2
```

- ✚ En cas d'usurpation d'adresse MAC (accès d'une MAC non autorisées à l'interface), plusieurs politiques de sécurité peuvent être envisagées.

- ▶ **Blocage du port**

Switch(config-if)# **switchport port-security violation shutdown**

- ▶ **On bloque toutes les trames avec des adresses MAC non connu et on laisse passer les autres. Le port ne se bloque pas suite à un accès non autorisé.**

Switch(config-if)# **switchport port-security violation protect**

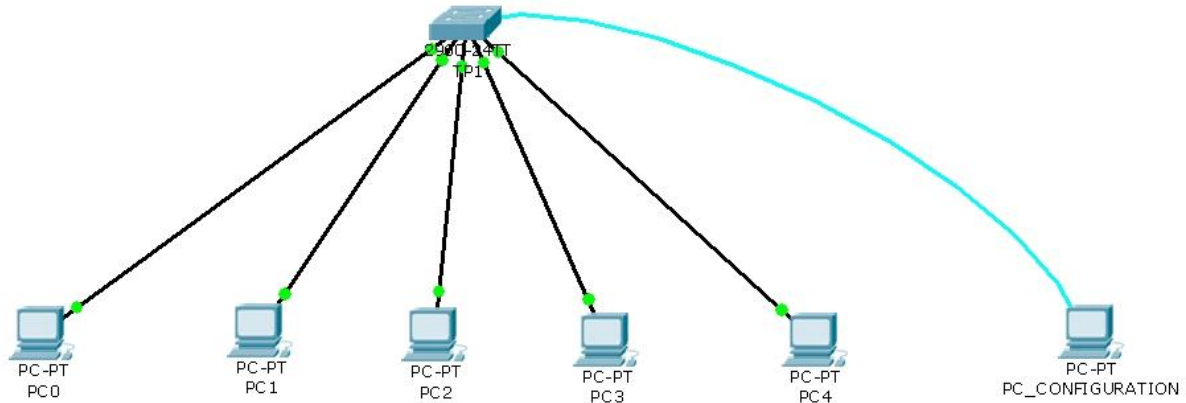
- ▶ **Soit un message dans le syslog et via SNMP sont envoyés. De plus le compteur du nombre de violation est incrémenté.**

Switch(config-if)# **switchport port-security violation restrict**

NB : les deux dernières options ne sont pas prises en charge par le simulateur.

Travail Demandé – PARTIE A

Tout d'abord à l'aide de l'outil de simulation schématiser le réseau de la figure ci-dessous.

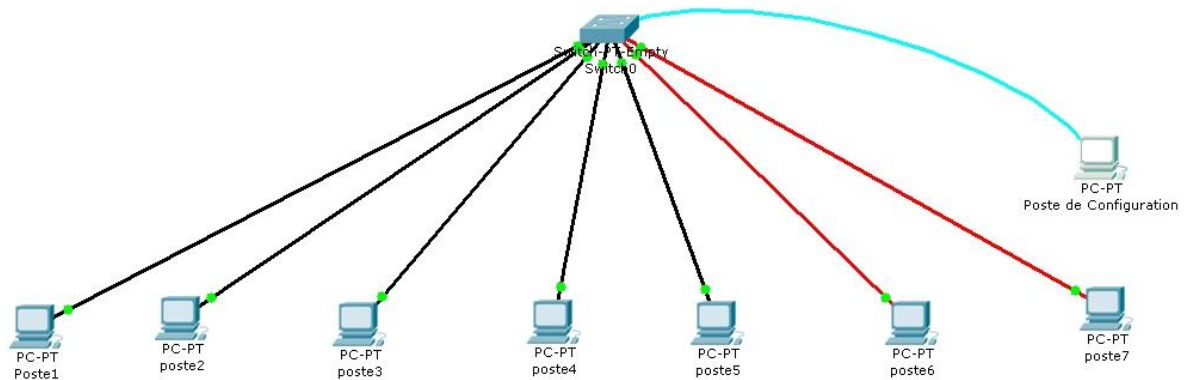


- Le switch choisi sera : le 2960 de la famille 2900 ;

1. Attribuer les adresses IP aux différents postes. Ceux là appartiennent au réseau 192.168.1.0. N'attribuer pas une adresse IP au poste de configuration ;
2. A partir du poste de configuration, accéder à la console du switch par le port série en utilisant l'outil Terminal. Expliquez le fait que même si le poste de configuration n'a pas une adresse IP, il peut se connecter via le port série à la console du switch.
3. Afficher la configuration courante ;
4. Donner le nom TP-partie1 au switch;
5. Utiliser la commande *show interfaces*, examiner en détail le résultat affiché ;
6. Utiliser la commande *show interfaces* pour une interface particulière : l'interface à laquelle est connecté PC0 ;
7. On considère l'interface **FastEthernet0/1** :
 - Désactiver cette interface ;
 - La réactiver ;
 - Mettre le mode duplex respectivement en half, full et automatique ;
 - Mettre la vitesse du port respectivement en 10 et 100 et automatique.
8. Attribuer une adresse ip au switch, qui doit appartenir au réseau 192.168.1.0. Essayez en premier lieu de donner au switch une adresse IP qui a été déjà attribuée à un poste et vérifier si cela est accepté ou non ;
9. Faites un ping vers le switch à partir d'un autre poste, vérifier que celle là aboutit ;
10. Examiner la configuration actuelle ;
11. Examiner la configuration de démarrage, et notez les différences.

Travail Demandé – PARTIE B

Schématiser le réseau de la figure ci-dessous.



- On considère le switch générique vide. Ajouter les modules du switch et les différentes cartes réseaux nécessaires aux postes, afin d'obtenir la connectivité suivante :

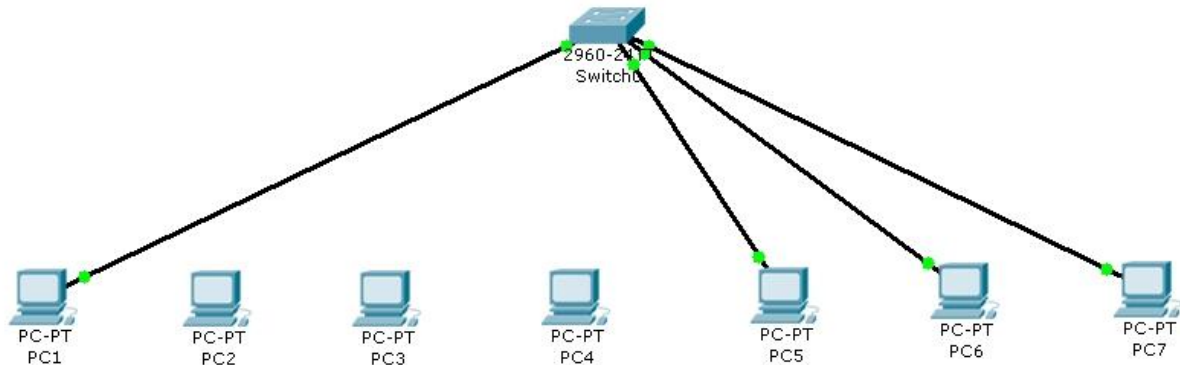
- le poste 1 est connecté à un port Ethernet à 10 Mbps ;
- les postes 2, 3 et 4 sont connectés à des interfaces Fast Ethernet sur paire torsadée;
- le poste 5 est connecté à une interface Gigabit Ethernet sur Paire torsadée ;
- le poste 6 est connecté à une interface Fast Ethernet sur Fibre Optique ;
- le poste 7 est connecté à une interface Gigabit Ethernet sur Fibre Optique ;

1. Attribuer les adresses IP aux différents postes. Ceux là appartiennent au réseau 192.168.1.0 ;
2. Connecter le poste de configuration au switch via le port série pour le configurer et lancer le terminal ;
3. Afficher la configuration courante ;
4. Afficher la configuration de démarrage ;
5. Quelle est la différence entre les deux configurations ;
6. Afficher les différentes interfaces et examiner comment elles sont nommées (show interfaces) ;
7. Donner le nom TP-partie2 au switch ;
8. Attribuer une adresse ip au switch ;
9. Afficher la configuration courante ;
10. Afficher la configuration de démarrage ;
11. Quelle est la différence entre ces deux configurations ;
12. Définir le mot de passe enable (vous pouvez spécifier un mot de passe au choix) ;
13. Revenir en mode utilisateur ;
14. Passer en mode privilège et vérifier que le mot de passe a été demandé ;

15. Définir un mot de passe au choix **secret** (vous pouvez spécifier un mot de passe au choix mais différents du mot de passe **enable**) ;
16. Revenir en mode utilisateur ;
17. Passer en mode privilège, lequel des mots de passe est demandé ?
18. Afficher la configuration courante. Que remarquez vous (de point de vue affichage des mots de passe d'accès : en clair ou cryptés) ;
19. Quitter la configuration du switch ;
20. Eteindre le switch et le redémarrer ;
21. Accéder via console à partir du poste de configuration et passer en mode privilège. Afficher la configuration courante, que remarquez vous ?? Est-ce que les mots de passes sont demandés ? Quelle est la raison?
22. Refaire toute la configuration (adresse ip du switch et le nom du switch, les mots de passes de mode enable et secret) ;
23. Enregistrer la configuration courante dans la configuration de démarrage ;
24. Quitter la configuration, éteindre le switch et le redémarrer ;
25. Vérifier que les paramètres configurés sont encore valides.
26. Définir les mots de passe d'accès via console ;
27. Se déconnecter du terminal virtuel ;
28. Connecter vous à travers le terminal virtuel, vérifier que le mot de passe est demandé ;
29. Définir le mot de passé d'accès via terminal ;
30. Afficher la configuration courante ; vérifier que les mots de passe sont affichés en clair ;
31. Crypter l'affichage des mots de passe ;
32. Afficher la configuration courante et vérifier que les mots de passes sont affichés cryptés ;
33. Afficher la configuration de démarrage, vérifier les différences ;
34. Sauvegarder la configuration courante dans celle du démarrage ;
35. Fermer la connexion terminal console ;
36. Eteindre le switch et ensuite le redémarrer ;
37. A partir du poste 4, connecter vous au switch via le terminal telnet. Vérifier que le mot de passe est demandé ;
38. Afficher la table des adresses mac du switch ;
39. Effacer la table des adresses mac ;
40. Faites un ping depuis le poste 1 vers le poste 5. Afficher la table des adresses mac du switch.. Qu'est ce que vous remarquez, déduire comment se fait l'apprentissage de la table des adresses mac au niveau du switch ;
41. Ajouter une adresse mac statique et ré afficher la table mac ;
42. Afficher la table arp. Quelle est la différence entre cette table et la table MAC ;
43. Sauvegarder la configuration courante dans la configuration de démarrage ;
44. Eteindre le switch.

Travail Demandé – PARTIE C : Contrôle d'accès

Mettre en place la topologie suivante, en utilisant un switch de type 2960 ;



1. Attribuer les paramètres IP aux postes PC1 → PC7. Nous allons considérer un adressage de classe C ;
2. Activer la sécurité sur le port auquel est connecté PC1. Dans toutes les questions qui suivent, nous allons considérer ce port ;
3. Faites la configuration nécessaire de façon que la première adresse MAC qui traverse ce port du switch soit la seule à être autorisée d'y accéder (adresse sticky) ;
4. Depuis PC1 faites un ping vers le PC5 ;
5. Examiner la configuration de sécurité sur cette interface. Quel est le nombre max de macs autorisés ;
6. Faites un ping à partir du PC1 vers le PC5, est ce qu'il aboutit ;
7. Changer le PC1 par le PC2 (débrancher PC1 de l'interface et brancher PC2) ;
8. Faire un ping à partir du PC2 vers le PC5 et vérifier si ça aboutit ou non. Quelle est la raison ?
9. Vérifier si l'interface est active. Quelle est la raison ? Si elle est inactive l'activer.
10. Rendre le nombre max de mac autorisée=3
11. Ajouter les adresses mac des postes PC3 et PC4 comme adresses mac autorisées;
12. Examiner la config de sécurité et vérifier le nombre d'adresses autorisées ;
13. Faites un ping à partir du poste PC2 vers PC5 et vérifier que c'est stoppé au niveau du switch ;
14. Ajouter l'adresse mac du PC2 à la liste des macs autorisés. Expliquer le résultat retourné.
15. Afficher la configuration de sécurité de ce port et voir le nombre de viols et l'adresse qui a fait le dernier viol ;
16. Quel est l'état de l'interface. Pour quelle raison elle est bloquée ;
17. Réactiver le port ;
18. Changer le poste PC2 respectivement par PC1, PC3 et PC4. Pour chacun de ces postes faites un ping vers le poste PC5. Est-ce que ces requêtes aboutissent, quelle est la raison ?

19. Retirer l'adresse MAC du PC4 de la liste des macs autorisés et ajouter l'adresse du poste PC2.
20. Faites un ping à partir du poste 4 et vérifiez si ceci parvient à destination ;
21. Si l'interface est bloquée, réactivez-la ;
22. Débranchez le poste PC4 et branchez le poste PC2, faites un ping vers le poste 5, est-ce que ça aboutit ? Pourquoi ça n'a pas abouti dans la tentative précédente et a abouti maintenant ?
23. Désactivez la sécurité sur le port et effacez la table des adresses mac.